Microsoft®

Windows®

Operating Systems

Microsoft Virtual Private Networking Security

White Paper

Abstract

This white paper provides an overview of the security issues surrounding implementation of Virtual Private Networks (VPNs) using the Microsoft® Windows® family of operating systems. In the Windows 95, Windows 98, and Windows NT 4.0 operating systems, Microsoft provides Virtual Private Networking (VPN) support through the Point-to-Point Tunneling Protocol (PPTP). To respond to reported issues and to enhance PPTP security, Microsoft has recently released enhancements to PPTP. With the release of the Windows 2000 operating system, Microsoft will broaden its VPN protocol support to include support for Layer 2 Tunneling Protocol (L2TP), as well as Internet Protocol Security (IPSEC) and the Extensible Authentication Protocol (EAP). This document describes these technologies, in addition to addressing security threats and countermeasures.

© 1999 Microsoft Corporation. All rights reserved.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Due to the nature of ongoing development efforts and because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft, the BackOffice logo, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other product or company names mentioned herein may be the trademarks of their respective owners.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

0299

CONTENTS

INTRODUCTION....1

VPN SECURITY BASICS....3
Supporting Front-End Processors 3
Voluntary and Compulsory Tunnels 4
Voluntary Tunneling 4
Compulsory Tunneling 4

USING PPTP VPNS....5
Providing Real-World Security 5
Evolving the Technology 5
Authentication Enhancement with MS-CHAP Version 2 6
Option to Require Stronger Password Authentication 7
Encryption Enhancement with MPPE 8
Control Channel Protection 9
What Customers Should Do 9

TUNNELING WITH L2TP....10
Tunneling with IPSec 10
IPSec Authentication 11

EXTENSIBLE AUTHENTICATION PROTOCOL....12
Transaction-Level Security (TLS) 12
RADIUS Authentication 13
RADIUS Accounting 13
EAP and RADIUS 13

CERTIFICATES....15
Machine Certificate Authentication 15
User Certificate Authentication 16
Active Directory Integration 16

ENCRYPTION....17
Symmetric (Private Key) Encryption 17
Asymmetric (Public Key) Encryption 17
Stateful and Stateless Encryption 17
IPSec and Stateless Encryption 18

FILTERING....19
Filtering in a VPN-R/RAS Server 19
IPSec Filtering 19
VPNs and Firewalls 19

ENHANCING SECURITY WITH NETWORK ADDRESS TRANSLATORS.21

CHOOSING YOUR VPN SOLUTION.....22
Performing a Risk Analysis 22
Increasing Security Through Password Policy 22
Looking Toward the Future 23

SUMMARY.....24

FREQUENTLY ASKED QUESTIONS ABOUT VPN SECURITY.....25
Is Windows NT 4.0-based Virtual Private Networking secure? 25
Are there other aspects of security that I should consider when making a decision about a VPN solution? 25
Are the security issues different for RAS than for VPN access? 25
What security features are built into PPTP? 26
How is PPTP secured? 26
What types of attack are used against VPNs? 26
What has Microsoft done to protect against attacks? 27
Dictionary Attacks 27
Server Spoofing 27
Weak Encryption Keys 28
Repeated Use of the Same Encryption Key 28
MPPE Key Synchronization 28
Bit-Flipping 28
PPP Negotiation Spoofing 29
Passive Monitoring 29
How important is good password security? 29
Are IPSec-based VPNs more secure than PPTP-based VPNs? 30
Are L2TP-based VPNs more secure than PPTP-based VPNs? 30
Is VPN outsourcing secure? 31
Is a server-to-server based VPN solution more secure than a client-server solution? 31
What are smart cards? 31
Does Microsoft support smart card authentication for VPNs? 31
What are token cards? 31
What are the tradeoffs between smart cards, token cards, and password-based security? 32

FOR MORE INFORMATION.....33

INTRODUCTION

The Microsoft® Windows® 95, Windows 98, and Windows NT® operating systems provide easy, secure, and economical communications enabling business without boundaries. One of the features of a Windows-based communications platform is Virtual Private Network (VPN) support.

VPNs have proven popular because they offer operational savings while maintaining the security associated with private network infrastructure. Using a VPN, a traveling worker or branch office can be connected to the corporate network with a local phone call, providing significant savings over using long distance, 800 numbers, or leased lines. Security is maintained because the VPN uses a secure *tunneled* connection, allowing only authenticated users access to the corporate Intranet. Microsoft's VPN solutions offer 128-bit encryption within the United States, with 40-bit encryption supported overseas where permitted by law. A Virtual Private Network can be described as the ability to *tunnel* through the Internet or other public network in a manner that provides the same security and other features formerly only available on private networks. With tunneling, a message packet is encapsulated within an IP packet for transmission across the public network, with the encapsulating information being stripped off upon arrival at the target network, such as the corporate local area network (LAN).

VPNs are so important to organizations supporting telecommuters, branch offices, and off-site partners, that VPNs are becoming a critical part of corporate Information Technology strategy.

Microsoft has pioneered integration of VPN solutions, and continues to work with industry partners and the Internet Engineering Task Force (IETF) to evolve the technology and security of virtual private networks. This paper looks at VPN security, the continuum of security challenges, and the different ways in which Microsoft VPNs provide security solutions.

Microsoft VPN solutions cover a spectrum of security needs. The Point-to-Point Tunneling Protocol (PPTP), which is available from Microsoft for the Windows 95, Windows 98, and Windows NT 4.0 operating systems, as well as on Windows 3.1 and Macintosh from third parties, was designed to provide the lowest Total Cost of Ownership. PPTP runs well on a wide variety of hardware, supports password authentication, and does not require implementation of a certificate infrastructure, although certificate support will be available in the Windows 2000 time frame.

Microsoft's implementations of Layer 2 Tunneling Protocol (L2TP) and Internet Protocol Security (IPSEC), which will be available on the Windows 2000 platform, are designed to provide the highest possible security. Consequently, these VPN solutions require deployment of a Public Key Infrastructure, and require a Pentium-class processor.

VPN SECURITY BASICS

This paper is intended to assist network administrators and other decision-makers in assessing the VPN security needs of their organization and choosing the solution that best fits their needs. The paper will also look at the role that security policy and employee education play in protecting a network, regardless of the technology deployed.

Securing a network is a dynamic, rather than a static challenge. All security represents a balancing act between protecting against potential security threats while not bogging down network or organizational performance.

Microsoft is committed to evolving its technology to provide the most powerful security solutions, while making the technology easy to deploy and manage.

The robust security of Microsoft VPN solutions allow organizations to take advantage of the convenience and cost savings of tunneling through public networks, without opening the door to unauthorized access.

A VPN tunnel works by encapsulating data within IP packets to transport information that does not otherwise conform to Internet addressing standards. These encapsulated packets are then transported between one network, or single client, and another network over an intermediate network. This entire process of encapsulation and transmission of packets is called tunneling, and the logical connection through which the packets travel is called a tunnel. A tunnel is a connection through the Internet or other intermediary network. The result is that remote users become virtual nodes on the network into which they have tunneled.

From the user’s perspective, the nature of the physical network being tunneled through is irrelevant because it appears as if the information is being sent over a dedicated private network.

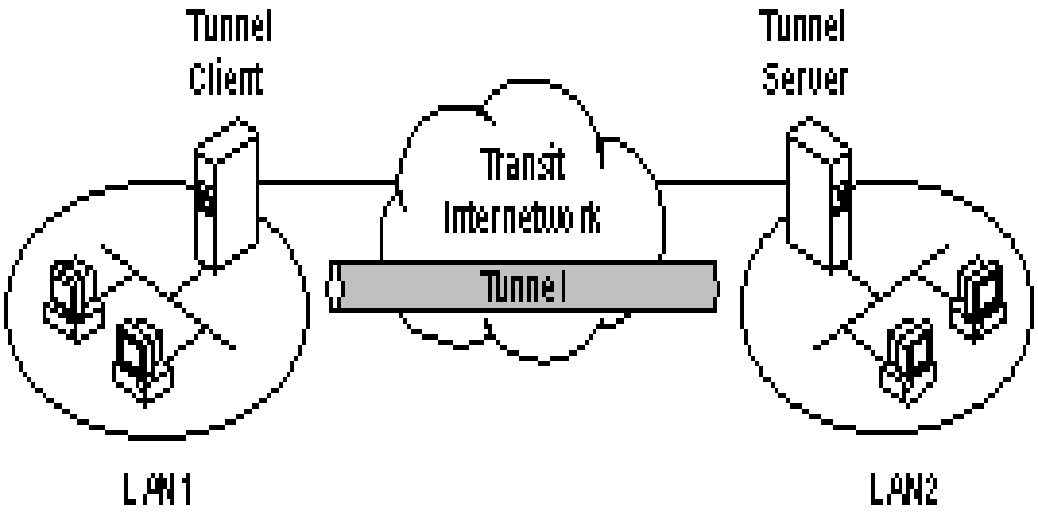

Figure 1. A conceptual model of a VPN.

Communication across the Internet requires both encapsulation and data stream encryption to be viable. Both PPTP and L2TP provide encapsulation services, to facilitate multiprotocol communications over the Internet. Encapsulation lets non-IP-based data packets communicate across the IP-based Internet from a remote client to a private corporate LAN, which allows non-IP-based networks to take advantage of the Internet.

Supporting Front-End Processors

Microsoft VPNs are designed to allow front-end processors (FEPs) to be connected with servers running Windows NT Server, so clients that call into the FEP have transparent access to the server's network. This means that even clients which aren't VPN-enabled can make tunneled connections, without even noticing whether they are going straight to the server, or to an FEP that is tunneling through the server. Because Microsoft VPN provides transparent access to a PPP client, it can work with UNIX, Win 16, the MS-DOS® operating system, Macintosh, and other clients.

An FEP can be operated by an Internet Service Provider because FEPs don't allow access to the data exchange between the client and server. The FEP is just a pass-through that lacks the intelligence to evaluate the information passing through it. From a security standpoint, this means a company will not lose control of who gets access to its network. Data privacy is maintained. This is very important for companies that outsource dial-up access because they need their data to be secure.

Another important point is to keep control of who has access to the server on the server itself, rather than on the FEP. The server authenticates the clients calling in. The FEP only looks at the caller's

identity and establishes the tunnel to the server. Because it has a passive role, security is tight.

Voluntary and Compulsory Tunnels

There are two kinds of VPN tunnels—voluntary and compulsory. Voluntary tunnels require the client to be VPN-enabled, whereas compulsory tunnels are used when the client instead relies upon a VPN-enabled FEP.

Voluntary Tunneling

Voluntary tunneling is a methodology in which the client workstation volunteers to create the tunnel to the target network. For this tunneling to occur, the client must be VPN-enabled with either PPTP or L2TP protocols and supporting software. (The tunnel server is always supplied with this protocol support.) The client and the server must both use the same tunneling protocol.

With voluntary tunneling, the client may already have a network connection that can provide transport between the workstation and its chosen tunnel server. More commonly, the workstation may have to establish a dial-up connection to the transport network before the client can set up a tunnel.

Compulsory Tunneling

If a client wishes to tunnel across the Internet, but is not VPN-enabled, it may be able to connect to a VPN-enabled FEP at an ISP. In the case of compulsory tunneling, the client can operate without L2TP or PPTP support software. These protocols are implemented at the FEP. The FEP and the tunnel server must, of course, support and use the same VPN protocol (PPTP or L2TP) for any specific connection.

Ordinarily, the user at the client machine is given a special phone number to dial up the FEP. For example, a corporation that owns the private network may have contracted with an ISP to assemble a nationwide set of FEPs. These FEPs can establish VPNs across the Internet to a tunnel server on the corporation’s private network. This configuration is known as *compulsory* tunneling because the client is compelled to use the VPN. Once the initial connection is made, the client is automatically routed into the tunnel.

Microsoft uses the Point-to-Point Tunneling Protocol to provide a very robust and secure virtual private networking solution. The ease of deployment and tight security of Microsoft’s PPTP-enabled VPN technology has made it the most preferred tunneling method in the industry, according to a 1998 VPN market study by Infonetics Research.

PPTP is an open industry standard. The specification for PPTP is the result

of joint efforts with a host of respected networking vendors including Ascend Communications, 3Com/Primary Access, ECI Telematics, US Robotics, and Microsoft. These companies constituted the PPTP Forum, whose joint effort was made publicly available and submitted to the IETF standards organization in 1996.

PPTP is integrated with the Remote Access Services server, which is built into Windows NT Server, and Windows 98, and is a component of the Dial-Up Networking 1.2 Upgrade for Windows 95.

Providing Real-World Security

All networking communication and security specialists realize that in real-world scenarios, computer security is a function of several dynamic elements including technology, policy, and physical security. It is within this framework, and after careful evaluation of their resources, that each organization defines its level of acceptable risk and the solutions it deploys. PPTP plays a part of an overall operational plan for secure communications, and is rooted in a pragmatic real-world approach to security issues–and is used by Microsoft for VPN connections to its own corporate networks.

Within a real-world context, Microsoft has not been contacted by any of its customers about a single case in which a Windows-based VPN communication has been compromised. However, despite this track record Microsoft continues to improve its Windows Networking and Communications technology with the recent release of the PPTP Performance and Security Upgrade for both Windows-based clients and servers. This is freely available form the Microsoft Communications Web site at http://www.microsoft.com/communications.

Microsoft's PPTP-enabled VPN solution combines the benefits of a broadly available open platform, full-featured networking, native Windows integration, and ease of use to deliver a highly programmable and flexible communications platform. A properly configured Windows-based system, using PPTP and Windows tools to enforce responsible password security policy, provides an economical, reliable, and secure VPN solution that delivers cost savings associated with Internet-based communications.

Evolving the Technology

Microsoft takes security very seriously. As a result of continual expert review, and rapid technological advancements, the state of the art in encryption and network security constantly changes. For this reason, Microsoft regularly provides prompt updates to its security services and products that rely on them. Customers charged with security policy should always be aware of the latest security enhancements available

from Microsoft, and should be regular monitors of the Microsoft security Web site at http://www.microsoft.com/security and the communications Web site at http://www.microsoft.com/communications.

Recent developments with Microsoft PPTP VPN technology include:

- Authentication Enhancement with MS-CHAP version 2
- Option to Require Stronger Password Authentication
- Encryption Enhancement with Microsoft Point-to-Point Encryption (MPPE)

Authentication Enhancement with MS-CHAP Version 2

Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP) is an authentication mechanism used to validate user credentials against Windows NT domains, while the resulting session keys are used to encrypt user data, as described below in discussing MPPE.

Encryption is the process of encoding data to prevent unauthorized access, especially during transmission. Encryption is accomplished by using a special algorithm together with a secret (also called a *key*) to transform data, such as a password, in such a way that the data cannot be understood by anyone who doesn't know the right key. The hashed password can only be decrypted by a computer that has been given the same key–rather like two kids having the same decoder rings, but using algorithms that make it all but impossible to break the encryption, especially on longer 128-bit keys.

MS-CHAP version 2 includes a one-way function of the user's password, a server-generated challenge, a client-generated challenge, and additional data in the MS-CHAP version 2 *Success* message. The MS-CHAP version 2 client disconnects if it cannot authenticate the server.

When the network access server receives an MS-CHAP version 2 authentication request from a remote client, it sends a challenge, which consists of a session ID and an arbitrary challenge string, to the remote client. The remote client must return the user name and hash of the challenge string, the session ID, and the hashed password. This design, which manipulates a hash of the hash of the password, provides an additional level of security because it allows the server to store hashed passwords instead of clear-text passwords.

MS-CHAP version 2 also provides additional error codes, including a password-expired code, and additional encrypted client-server messages that permit users to change their passwords. In Microsoft's implementation of MS-CHAP version 2, both the client and the server independently generate an initial key for subsequent data encryption by MPPE.

Previously, Microsoft PPTP VPNs could be configured to accept less

demanding authentication protocols. To enhance security during authentication, Microsoft PPTP now uses only MS-CHAP.

Option to Require Stronger Password Authentication

As noted above, when Windows-based clients connect to a Windows NT-based PPTP server, they perform a challenge-response authentication by using a technique called MS-CHAP. This technique uses a hashing function to obscure the Windows NT password in the response. (A Windows NT password is case-sensitive, can be up to 14 characters long, and uses the 16-bit Unicode character set.)

Because authentication is based, in part, upon the hashing of the user's password to generate the initial encryption keys, network administrators should enforce use of the more complex Windows NT password structure. Theoretically, knowledge of the user's password could allow a malicious attacker who was able to sniff the network between the client and server to decrypt the data in the encrypted PPTP session. (This becomes even more difficult with the 128-key encryption algorithm as the password is only part of the information hashed to create the key.)

Although older LAN Manager (LM) passwords can be used, LM passwords are not as complex as Windows NT passwords, and thus are more susceptible to brute force or dictionary attacks, in which an intruder attempts to guess a user's password.

Requiring Use of Windows NT Passwords

Microsoft has released an update to the PPTP client and server components for Windows NT that provides administrators with the ability to configure the PPTP server so that it will only accept the stronger password authentication of Windows NT. This update also allows the administrator to configure Windows NT-based PPTP clients such that they will never use LM authentication. Shortly, Microsoft plans to release an update to the Windows 95-based PPTP client that will allow the Windows 95-based client to be configured such that it will never use LM authentication when connecting to PPTP servers. Windows 98 already includes this updated functionality. Specific information regarding the update and how to configure Windows to mandate the use of the Windows NT Hash is covered in the release notes of the upgrade software. Please see http://www.microsoft.com/communications/ for information on the updated release for Windows 95, Windows NT, and the integrated Routing and Remote Access Services of Windows NT Server for server-to-server VPN.

Enforcing Password Policy

Microsoft recommends that customers enforce the use of strong (complex) passwords on their networks by using the tools in Windows that allow an administrator to do so. Passwords should mix uppercase

and lowercase letters, numbers, and punctuation. A good password policy that specifies minimum password length, character diversity, and regular updating is an important part of maintaining network security.
Windows NT can easily enforce such a password policy. Service Pack 2 for Windows NT 4.0 and subsequent service pack releases provide tools for Windows NT administrators to enforce better security policy through improved password management.

Basics of Good Password Policy

As noted above, strong passwords require at least a minimum number of characters and a diversity of character types. Good passwords should also be unguessable by others. This is critical because poorly chosen passwords harm security.

Poorly chosen passwords include those which:

- Are made up solely from dictionary words.
- Are only one case (upper or lower).
- Are created from names of people or things that could be guessed by others, such as the name of a user's child, pet, or even mother's maiden name.

Well-chosen passwords include those which:

- Contain at least one number and one symbol (such as a *?*) in the middle.
- Appear to be "gobbledygook" to the casual observer.
- Do not contain dictionary words or proper names.

Microsoft Knowledge Base article Q161990 provides information about enabling strong password policy within an organization. Good password policy management makes any password-based solution exponentially more difficult to compromise. Complex passwords, good technology, and the constraints of the physical world all combined to make Windows a very secure real-world VPN solution.

Please also note that in Microsoft's 128-bit encryption algorithm, the encryption key is not just a function of a complex password, but also includes a function on the challenge. This algorithm makes an attack much more difficult. Microsoft recommends the use of 128-bit encryption keys for North America as a matter of policy, not just for protection against an attack, but also because 40-bit keys have been shown to be susceptible to brute force attacks under controlled conditions.

Encryption Enhancement with MPPE

Using encryption provides an additional layer of security for PPTP-based virtual private networks. Although this is rarely, if ever, seen in the real world, it is theoretically possible for a person to intercept VPN packets. If an attacker could position a machine between the client and its target server, the machine in the middle could attempt to impersonate the

subject PPTP server and accept the traffic from the client. The vulnerability to *man-in-the-middle* attacks exists with any non-mutual challenge-response authentication protocol, and is therefore not specific to Microsoft's products. In addition, MS-CHAP version 2 provides mutual authentication and was specifically designed to defeat just such an attack.

Using MPPE 128/40-bit software-based encryption, all user data communicated between the client and the server is fully protected and cannot be read by the machine in the middle that lacks the necessary key to decrypt information transmitted.

PPTP uses the RSA RC4 encryption algorithm, operating at the strongest encryption level allowed by the U.S. government—using 128-bit keys in North America, and 40-bit keys elsewhere. When MS-CHAP version 2 is used, separate RC4 encryption keys are derived for each direction, and by default, the encryption keys are changed on every single packet. These facts make even well-resourced brute force attacks extremely difficult.

Control Channel Protection

A bug found and reported to Microsoft several months ago would have allowed a malicious attacker to send flawed information to the PPTP server over what is called the control channel. This code, if constructed properly, could potentially have caused the PPTP server to crash. Microsoft has released a publicly available fix for this bug. This fix provides more extensive parameter checking on data passed to the control channel to ensure that data in the control channel can not crash the PPTP server. This fix is also included in the recently released PPTP updates for Windows NT. Microsoft Knowledge Base article Q179107 provides more information about this resolved bug.

After this fix, the worst result of an attack of this type would be the dropping of an active PPTP session. To eliminate such attacks, Microsoft plans to further enhance the PPTP control channel in a future update to fully authenticate each control channel packet sent to a PPTP server.

What Customers Should Do

North American customers should continue to use the strong 128-bit version of PPTP on their networks. Customers should also update to the latest service pack for Windows NT 4.0 and install the latest PPTP hotfixes.

In general, customers should regularly review the Microsoft Security Web site at http://www.microsoft.com/security, and Windows Communications Web site at http://www.microsoft.com/communications. Customers should then load and use the latest security information, advisories, and

updates for both the Routing and Remote Access Services that enable server-to-server and the latest dial-up networking upgrades for client-to-server VPNs. Users should then make sure that their organization uses the tools provided to enforce a responsible security policy. Properly configured Windows-based systems, combined with a good security policy, ensure that you can reap all the benefits of a secure VPN solution.

The Layer 2 Tunneling Protocol is a technology that combines the best of PPTP and Layer 2 Forwarding (L2F). L2F is a proposed transmission protocol that allows dial-up access servers to frame dial-up traffic in PPP and transmit it over WAN links to an L2F server, which then unwraps the packets and injects them into the network.

L2TP provides tunneling over any media that provides packet-oriented point-to-point connectivity, which includes WAN technologies such as X.25, Frame Relay, and ATM. L2TP also provides the ability to establish multiple tunnels between two tunnel endpoints. (L2TP is documented in "Layer Two Tunneling Protocol - L2TP," published as draft-ietf-pppext-l2tp-12.txt. The most recent version of this document can be found on the IETF Web site, http://www.ietf.org/.)

When used over IP internetworks, L2TP is very similar to PPTP. An L2TP tunnel is created between an L2TP client and an L2TP server. The client may already be attached to an IP internetwork (such as a LAN) that can reach the tunnel server, or a client may have to dial into a network access server (NAS) to establish IP connectivity (for dial-up Internet users).

Both PPTP and L2TP use PPP to provide an initial envelope for the data and then append additional headers for transport through the transit internetwork. Some differences between PPTP and L2TP:

- PPTP requires that the transit internetwork be an IP internetwork. L2TP requires only that the tunnel media provide packet-oriented point-to-point connectivity. L2TP can be run over IP (using UDP), Frame Relay PVCs, X.25 VCs, or ATM VCs.
- PPTP can only support a single tunnel between endpoints. L2TP allows for the use of multiple tunnels between endpoints.
- L2TP provides for header compression, documented in draft <<insert here>>. When header compression is enabled, L2TP operates with 4 bytes of overhead, compared with 6 bytes for PPTP.
- L2TP provides for tunnel authentication, whereas PPTP does not. However, when either PPTP or L2TP is run over IPSec, tunnel authentication is provided by IPSec so that Layer 2 tunnel authentication is not necessary.

Creation of L2TP tunnels must be authenticated using the same authentication mechanisms as PPP connections. L2TP inherits encryption

and/or compression of PPP payloads from PPP, and additional encryption security can be added by implementing IP Security (IPSec), described in the following section.

Tunneling with IPSec

Internet Protocol Security (IPSec) was designed by the IETF as an end-to-end mechanism for ensuring data security in IP-based communications. IPSec has been under development and analysis by some of the best people in network security for several years. It is a scheme that authenticates and encrypts IP packets on an individual basis. It is believed to be highly secure. However, IPSec was originally designed to provide protection on a machine-to-machine basis (in particular, to protect traffic traveling between routers on the Internet). Today, IPSec more or less assumes that each host has a static IP address.

IPSec has been defined in a series of request for comments (RFCs), notably RFCs 1825, 1826, and 1827, which define the overall architecture; an Authentication Header for verifying data integrity; and an Encapsulation Security Payload for both data integrity and data encryption.

The primary focus of IPSec is on providing network-layer security for IP. IPSec integrates with the inherent security of the Windows NT Server operating system to provide an ideal platform for safeguarding intranet and Internet communications.

IPSec enables server-to-server tunneling, such as between routers, rather than being used for client-server tunneling. Therefore, it complements, rather than overlaps, the functionality provided by PPTP and L2TP. The flexibility of Layer 2 VPN protocols (PPTP/L2TP) can therefore be powerfully combined with the security provided by IPSec. Microsoft plans to support such a *merged VPN* platform (PPTP or L2TP running over IPSec) in Windows 2000.

In addition to its definition of encryption mechanisms for IP traffic, IPSec defines the packet format for an IP over IP tunnel mode, generally referred to as IPSec Tunnel Mode. An IPSec tunnel consists of a tunnel client and tunnel server, which are both configured to use IPSec tunneling and a negotiated encryption mechanism.

IPSec Tunnel Mode uses the negotiated security method (if any) to encapsulate and encrypt entire IP packets for secure transfer across a private or public IP internetwork. The encrypted payload is then encapsulated again with a plain text IP header, and sent on the internetwork for delivery to the tunnel server. Upon receipt of the datagram, the tunnel server processes and discards the plain text IP header and then decrypts its contents to retrieve the original payload IP

packet. The payload IP packet is then processed normally and routed to its destination on the target network.

IPSec Tunnel Mode supports IP traffic only, and it functions at the bottom of the IP stack. Therefore, applications and higher-level protocols inherit its behavior. It is controlled by a security policy, or set of filter-matching rules, which establishes the encryption and tunneling mechanisms available in order of preference and the authentication methods available, also in order of preference. As soon as there is traffic, the two machines perform mutual authentication, and then negotiate the encryption methods to be used. Thereafter, all traffic is encrypted using the negotiated encryption mechanism and then wrapped in a tunnel header.

IPSec Authentication

IPSec uses an authentication header and a sequence number to provide source authentication and integrity without encryption. IPSec uses the Encapsulated Security Payload (ESP) to provide authentication and integrity along with encryption. With IP Security, only the sender and recipient know the security key. If the authentication data is valid, the recipient knows that the communication came from the sender, and that it was not changed in transit.

The Extensible Authentication Protocol (EAP) is an extension to PPP, providing a standard support mechanism for authentication schemes such as token cards, Kerberos, Public Key, and S/Key, and is fully supported on both the Windows NT Dial-Up Server and the Dial-Up Networking Client. EAP is a critical technology component for secure VPNs, protecting them against brute force or dictionary attacks and password guessing.

EAP allows third-party authentication modules to interact with the Microsoft Windows NT Remote Access Service (RAS) VPN implementation. The availability of EAP on Windows NT is in response to increasing demand to augment RAS authentication with third-party security devices.

EAP is an IETF-proposed extension to PPP that allows for arbitrary authentication mechanisms to be employed for the validation of a PPP connection. EAP was designed to allow the dynamic addition of authentication plug-in modules at both the client and server ends of a connection. This allows vendors to supply a new authentication scheme at any time. EAP provides the highest flexibility in authentication uniqueness and variation. EAP is planned to be implemented in Microsoft Windows 2000.

Transaction-Level Security (TLS)

Smart cards and token cards can offer robust security for VPNs. Smart cards are small devices about the size of credit cards, which contain a CPU and a little memory. They are commonly used to store authentication credentials (such as public key certificates), encryption keys, and account information. Some also implement encryption algorithms on board, so that the encryption keys never leave the smart card. At present, smart cards are not widely used for remote access security, because few remote access packages support them. Windows 2000, however, will support the use of smart cards for all varieties of authentication, including RAS, L2TP, and PPTP.

Token cards from different vendors work in a variety of ways, but they are all basically hardware password generators. For example, some cards have a small LCD display and a keypad like a calculator. The user enters a numeric PIN, and the card displays a numeric passcode, which is then used as a password. Normally, token cards are designed so that they will only produce a given passcode once. Token cards work great for dial-up applications (like RAS) or host authentication. Because network applications of token cards are usually client-server based, token cards (and other on-time password schemes) can be vulnerable to eavesdropping.

These cards, and public key user certificates, will be supported through the use of Extended Authentication Protocol-Transaction Layer Security (EAP-TLS), which has been submitted to the IETF as a draft proposal for a strong authentication method based on public key certificates. With EAP-TLS, a client presents a user-certificate to the dial-in server, while at the same time, the server presents a server certificate to the client. The first provides strong user authentication to the server; the second provides assurance that the user has reached the server he or she expected. Both systems rely on a chain of trusted authorities to verify the validity of the offered certificate.

The user’s certificate could be stored on the dial-up client PC, or stored in an external smart card. In either case, the certificate cannot be accessed without some form of user identification (PIN number or name/password exchange) between the user and the client PC. This approach meets the “something you know plus something you have” criteria recommended by most security experts.

EAP-TLS is the specific EAP method that will be implemented in Windows 2000. Like MS-CHAP, EAP-TLS will return an encryption key to enable subsequent data encryption by MPPE.

RADIUS Authentication

Remote Authentication Dial-in User Service is a central authentication

database server in addition to an authentication request protocol. The RADIUS protocol is a UDP-based protocol that supports PPP, PAP, or CHAP; a UNIX logon feature, and other authentication mechanisms. RADIUS authentication also provides accounting capabilities.

The RADIUS server receives a user connection request from the NAS and authenticates the client against its authentication database. A RADIUS server also maintains a central storage database of other relevant user properties. In addition to the simple YES/NO response to an authentication request, RADIUS can inform the NAS of other applicable connection parameters for this user, such as maximum session time, static IP address assignment, and callback information.

RADIUS can respond to authentication requests based on its own database, or it can be a front-end to another database server such as a generic open database connectivity server or the primary domain controller. The latter server can be located on the same machine as the RADIUS server, or can be centralized elsewhere. In addition, a RADIUS server can act as a proxy client to a remote RADIUS server.

RADIUS Accounting

RADIUS allows centralized administration and accounting of multiple tunnel servers. Most RADIUS servers can be configured to place authentication-request records into an accounting file. There are also a set of messages from the NAS to RADIUS that request accounting records at the start of a call, the end of a call, and at predetermined intervals during a call. A number of third parties have written billing and audit packages that read RADIUS accounting records and produce various useful reports.

EAP and RADIUS

EAP used in combination with RADIUS requires changes to both the NAS and to RADIUS. For traditional authentication, the NAS/RADIUS interaction is a single request/response exchange. But in an EAP authentication, the NAS cannot collect client information for EAP authentication by RADIUS, because the information the EAP-enabled RADIUS needs is hidden from the NAS. To solve this problem, system administrators can configure the NAS to send an EAP identity message to the client, which sends the user name and domain data to the NAS. The NAS presents this data to RADIUS in an EAP-START request, and then becomes transparent to the remainder of the authentication process. RADIUS sends and replies to EAP messages through NAS to the client until authentication either succeeds or fails.

A certificate (or public key certificate) is a data structure that is digitally signed by a certificate authority (CA)—an authority that users of the certificate can trust. The certificate contains a series of values, such as

the certificate name and usage, information identifying the owner of the public key, the public key itself, an expiration date, and the name of the certificate authority. The CA uses its private key to sign the certificate. If the receiver knows the public key of the certificate authority, the receiver can verify that the certificate is indeed from the trusted CA, and therefore contains reliable information and a valid public key. Certificates can be distributed electronically (through Web access or e-mail), on smart cards, or on floppy disks.

Support for public key certificate authentication in Windows NT allows client applications to connect to secure services on behalf of users who do not have a Windows NT domain account. Users who can be authenticated based on a public key certificate issued by a trusted Certificate Authority can be granted access to Windows NT resources. The Directory Service administration tools allow administrators, or delegated authorities, to associate one or more external users to an existing Windows NT account for access control. The subject name in the X.509 version 3 certificate is used to identify the external user that is associated with the account.

Client accounts are validated against the Windows NT user database, and only those with valid permissions are allowed to connect. The keys used to encrypt data are derived from the user’s credentials, and are not transferred on the wire. When authentication is completed, the user's identity is verified, and the authentication key is used for encryption.

Businesses can share information in a secure manner to selected individuals from other organizations without having to create many individual Windows NT accounts. Many-to-one mapping of certificates to Windows NT user objects provides for strong authentication based on public key certificates and common access-control permissions. Client authentication of external users still requires the system administrator to configure the Certificate Authority for the external user’s certificates as a trusted CA. This prevents someone with a certificate issued by an unknown authority from authenticating to the system as someone else.

Machine Certificate Authentication

A machine certificate is used to validate a sender or receiver at a system level. Machine certificates differ from server certificates in that they represent the machine itself, and can be used for multiple services.

Although machine certificates identify a computer at a system level, they do not identify a specific user using that machine. Thus, for applications such as dial-in user authentication, user certificates, to be described later, are more secure because they identify the user rather than the client machine. This identity can then be used to provide secure access to resources.

ENCRYPTION

User Certificate Authentication

A user certificate is used for the validation of a specific user and to make the user's public key accessible for encryption/decryption functions. Elements of a user certificate are the user's name relative to a directory system (such as an X.500 user name), the user's public key, the name of the signing CA and the expiration date of the certificate.

User certificates can be stored on smart cards or on the user's computer. In both cases, they are usually protected from access by some form of password. They may also be stored in a directory system for comparison with the certificates presented by a user requesting network access.

Active Directory Integration

With Windows 2000, the Directory Service is used to publish public key certificates for users, and standard directory access protocols are used to locate them. Private keys and certificates issued to users are kept in secure storage, either on the local system or smart card. The secure storage is provided with the Internet security technologies and is known as a Wallet.

The implementation of the Wallet is based on Microsoft's CryptoAPI architecture for Windows NT. CryptoAPI provides key management functionality and other cryptographic functionality for building a secure store. The Windows NT implementation of public key-based security protocols will use keys and certificates stored in the Wallet as user credentials for accessing Internet-based servers. In many cases, user-defined properties of certificates in the Wallet allow the security protocols to automatically select and use the correct certificate and signature key. Advances in Internet security protocols (SSL3/TLS) allow a server to request specific credentials from the client that will be used automatically from the Wallet if they are available.

VPN security is enhanced through the use of encryption to protect passwords in addition to the content of data packets. The keys used to encrypt data are derived from the user credentials, and are not transferred on the wire. When authentication is completed, the user's identity is verified, and the authentication key is used for encryption.

Both PPTP and L2TP inherit optional encryption and compression protocols from PPP, and additional encryption security can be added by implementing the IPSec protocol, because the Microsoft implementation of L2TP allows for IPSec encryption. A number of encryption technologies may be used to provide data security with VPNs.

Symmetric (Private Key) Encryption

Symmetric, or private key, encryption (also known as conventional

encryption) is based on a secret key that is shared by both communicating parties. The sending party uses the secret key as part of the mathematical operation to encrypt (or encipher) plaintext to ciphertext. The receiving party uses the same secret key to decrypt (or decipher) the ciphertext to plaintext. Examples of symmetric encryption schemes are the RSA RC4 algorithm (which provides the basis for Microsoft Point-to-Point Encryption), Data Encryption Standard (DES), the International Data Encryption Algorithm (IDEA), and the Skipjack encryption technology proposed by the United States government for use in the Clipper chip.

Asymmetric (Public Key) Encryption

Asymmetric, or public key, encryption uses two different keys for each user: One is a private key known only to the user. The other is a corresponding public key, which is accessible to anyone. The private and public keys are mathematically related by the encryption algorithm. One key is used for encryption and the other for decryption, depending on the nature of the communication service being implemented. Public key encryption technologies also allow digital signatures to be placed on messages. A digital signature uses the sender's private key to encrypt some portion of the message. When the message is received, the receiver uses the sender's public key to decipher the digital signature—and verify the sender's identity.

With symmetric encryption, both sender and receiver have a shared secret key. The distribution of the secret key must occur (with adequate protection) prior to any encrypted communication. However, with asymmetric encryption, the sender uses a private key to encrypt or digitally sign messages, while the receiver uses a public key to decipher these messages. The public key can be freely distributed to anyone who needs to receive the encrypted or digitally signed messages. The sender needs to carefully protect the private key only.

Stateful and Stateless Encryption

When choosing encryption schemes, it is important to note the differences between stateful and stateless encryption.

With stateless encryption, each packet is self-sufficient and contains all the necessary information required to decrypt the packet. With stateful encryption, each packet relies on the previous packet or packets to successfully decrypt the packet.

The choice of stateless versus stateful encryption is a tradeoff between the strength of encryption and performance in high-loss environments, or environments without ordering support. Stateless encryption requires that each packet be decipherable as a stand-alone unit. This is less

strong than stateful encryption, in which knowledge from a previous packet is required in order to decipher any individual packet. But because the decryption of a packet is dependent on the arrival of the previous packet, stateful encryption loses one additional packet for every contiguous set of packets lost. So performance suffers in the face of lost packets or out-of-sequence delivery.

IPSec encryption mechanisms typically use stateless encryption methods for the simple reason that an IP network environment cannot guarantee packet delivery. PPP encryption mechanisms typically use stateful encryption because the point-to-point environment for which PPP was invented does guarantee packet delivery and correct sequencing.

IPSec and Stateless Encryption

IPSec encryption schemes encrypt each packet individually and do not depend on the encryption of previous packets. Therefore, the loss of a single packet will affect that packet only, but will not prevent other packets from being decrypted. When Layer 2 tunneling protocols (such as PPTP and L2TP) are run over IPSec, it is possible to use the IPSec stateless encryption mechanisms rather than the stateful encryption mechanisms of PPP.

IPSec builds upon the IETF model by mixing public key and secret key cryptography, and providing automatic key management for maximized security and high-speed throughput. This gives a combination of authentication, integrity, anti-replay, and—optionally—confidentiality, to ensure secure communications. Because Windows IP Security is below the network layer, it is transparent to users and existing applications. Organizations automatically get high levels of network security.

IPSec implementations typically offer support for a wider variety of encryption algorithms than do Layer 2 tunneling protocols, which are based on PPP encryption. However, when Layer 2 tunneling protocols are run over IPSec, all of the IPSec encryption algorithms become available to encrypt the Layer 2 tunneling traffic.

Filtering provides network managers with an important security feature. An administrator can decide to only allow authenticated VPN-enabled users to connect to the corporate network from the Internet. Filtering out non-PPTP or non-L2TP packets avoids the risk of somebody attacking the corporate network through the VPN gateway server. Filtering prevents all other packets from entering the private network. In combination with PPP encryption, this practice ensures that only authorized encrypted data enters or leaves the private LAN.

Filtering in a VPN-R/RAS Server

Microsoft Routing and Remote Access Server integrates routing with RAS and VPN support, can set packet filters on individual ports, and supports L2TP with Windows 2000.

In an R/RAS-VPN server, PPTP or L2TP filters can be applied to the tunnel server's input ports, thus blocking packets that do not conform to designated protocol specifications as implemented on the server. Such specifications could include packets whose destination address corresponds to a specified server, whose address is included within a set of source IP addresses, where valid private network addresses were assigned by the tunnel server, and where the private network source address is valid.

Filters can also be set on the tunnel server output ports to filter data packets as they *leave* the private network. For example, a scheme might be implemented for checking a packet's destination address against a set of acceptable addresses R/RAS maintains. Conversely, packet source addresses could be verified in the same way.

IPSec Filtering

IPSec can be envisioned as a layer below the TCP/IP stack. This layer is controlled by a security policy on each machine and a negotiated security association between the sender and receiver. The policy consists of a set of filters and associated security behaviors. If a packet's IP address, protocol, and port number matches a filter, then the packet is subject to the associated security behavior.

VPNs and Firewalls

Firewalls are another method of ensuring corporate network integrity by strictly regulating what data can enter the private network from the Internet. There are two approaches to using firewall techniques with a VPN.

A VPN tunnel server can be installed in front of a firewall, behind a firewall, or on the same machine. The most secure configuration calls for the VPN server to be placed in front of the firewall. Using Windows NT, the VPN tunnel would be configured to filter non-PPTP packets. Once the PPTP packets are filtered, they are decompressed and unencrypted. The communication is then passed to the firewall, where the firewall can provide further active filtering and screening services on the previously encapsulated and encrypted content. This approach, with the VPN server in front of the firewall, is the most secure configuration. It is the recommended configuration for either an extranet application of numerous trusted partners or if financial resources do not preclude consideration.

ENHANCING SECURITY WITH NETWORK ADDRESS TRANSLATORS

(Note Running the Routing and Remote Access Service in Windows NT Server can provide some static filtering to filter packets by source and destination addresses, protocol, port, or other filtering criteria. Although this can provide some incremental security, it is not to be understood as equivalent to a firewall solution).

As previously noted, a firewall can also be placed in front of the VPN server. This solution, although possible, results in more packets being analyzed by the server. In addition, there is incremental risk posed if the PPTP-based packets are being permitted to pass through to a VPN Server. These packets cannot be scrutinized by the firewall because they are both encrypted and compressed. The security risk posed by such a configuration is confined to that posed by an employee granted remote access. This internal risk is also faced each day if the employee has access to the LAN. This configuration, and the risks embodied in it, suffices for an intranet-like application.

Some organizations, due to constrained resources, may also wish to install the firewall on the same machine as the VPN server. Under this scenario, a single machine directs the VPN traffic to its specified destination and directs all other traffic received by the server to the firewall for analyses. This approach is the most economical and is recommended for *intranet* or company-specific communications.

A Network Address Translator (NAT) allocates private addresses to clients, which the NAT then translates into acceptable public IP addresses for Internet traffic. Some organizations use a NAT behind their firewall for the additional security that comes from not exposing their internal address structure.

NAT is typically installed as a component of multiprotocol routing. Two general types of NAT deployments exist. In the first type, a small LAN may have private addresses, and then receive a corresponding number of Internet addresses from InterNIC. A NAT is configured to map each private address to an individual Internet address, or vice versa. In the second case, the LAN has more private addresses than Internet addresses. A NAT establishes an internal address-mapping table. When a packet from a LAN client goes through the NAT to reach the Internet, the NAT changes the source address field of the packet. It keeps a record of the original client address in addition to a newly NAT-supplied and Internet-friendly source address field. The NAT then transmits the message to the Internet. When Internet messages are received at the NAT, the NAT uses its address translation table to re-map the source address field back to the original client, and sends the packet on its way.

L2TP gives Microsoft VPNs the ability to go through a network address translation, because it is layered on top of UDP. In contrast, PPTP is layered on top of generic routing encapsulation, which lacks the ability to work with NATs.

A joke in the computer security industry specifies that completely securing a computer is a two-step process:

1) Encase it in concrete.

2) Throw it off a pier.

The idea is that security is never absolute. But neither is the magnitude of the security *threat* absolute. And the good news is that the security provided by Microsoft PPTP-enabled VPNs and Microsoft Point-to-Point Encryption is secure. Microsoft and its employees utilize this technology on a daily basis to economically transmit private information securely over public and private networks.

With the Windows 2000 support of L2TP, the end-to-end protection of IP Security, the smart cards of Enhanced Authentication Protocol, and the use of Kerberos certificates, network administrators have a spectrum of Microsoft security solutions to choose from when deploying a VPN.

Performing a Risk Analysis

This is why a good first step is for a network administrator to perform a risk analysis to consider network vulnerabilities, the probability of an attack, and the consequence of a successful attack.

Another part of the analysis is to determine the impact of the solution. For example, a company considering a complete IP Security solution might need to upgrade all of its 486 or early Pentium computers to accommodate the additional CPU demands of supporting IP Security. For a network hosting applications involving extremely sensitive information and high likelihood of attack, the move to IPSec could be a wise investment. A business with less risk of attracting intruders might forgo the expense of upgrading machines and implement a PPTP VPN.

Microsoft support of the Enhanced Authentication Protocol in Windows 2000 allows companies to deploy smart cards or token card-based security systems in which users have to physically carry a credit card-like device to log onto their computers. The extra layer of security afforded should be weighed against the pragmatic real-world problems of people leaving their smart cards at home or losing them.

Similarly, the extra security provided by Kerberos certificates could be essential to some operations. But other network managers would be

hesitant to commit to the potentially huge undertaking of integrating their networks to support a public key infrastructure.

Increasing Security Through Password Policy

The ease of deployment and management, coupled with its tight security and support of MPPE data encryption, make Microsoft's PPTP-enabled VPNs one of the most widely used solutions in use. Again, each network administrator must determine a security solution that best matches their risk analysis, but for a large percentage of organizations, including Microsoft, PPTP-enabled VPNs provide the tight security required for safely deploying virtual private networks.

Although the password-based authentication of PPTP is easier to administer than smart cards or certificates, it is critical that network administrators protect the security of their PPTP VPNs (in addition to other network resources) through password policy that enforces:

- The use of Windows NT passwords.
- The use of complex character strings (upper and lower case, numerals, punctuation, and minimum length)
- Regular changing of passwords.

Good security policy also includes practical matters, such as reminding users not to conspicuously display their password, for instance, by taping it onto their monitor.

Looking Toward the Future

Microsoft is a leader in developing and implementing encryption and other security technologies. Because security is so crucial to maintaining the integrity of the world's computer networks, research and development at Microsoft and elsewhere is a continuing project. For example, the Internet Protocol Security Protocol Working Group is developing enhancements to IP security, and RSA Data Security is leading a consortium effort to implement the S/WAN initiative, to ensure interoperability among firewall and TCP/IP products. As new security technologies are developed, they will be evaluated for integration with Microsoft VPN.

Microsoft continues to evolve its Virtual Private Networking to provide users with well-integrated and secure VPN solutions. The Point-to-Point Tunneling Protocol lets organizations take advantage of the convenience and cost savings of tunneling through public networks, without opening the door to unauthorized access. Microsoft Point-to-Point Encryption provides the additional security of encrypting the tunneled data. Windows 2000 will provide the option of using the Layer 2 Tunneling Protocol, IP Security, and the Extensible Authentication Protocol to

support additional methods of authentication, such as smart cards.

Microsoft recognizes that security is a dynamic threat, and proactively responds to the changing demands of network security by continuously evolving the technology needed to provide secure network operations. This commitment has produced an even tighter PPTP VPN solution through improvements including:

- Authentication Enhancement with MS-CHAP
- Option to Require Stronger Password Authentication
- Encryption Enhancement with Microsoft Point-to-Point Encryption (MPPE)
- Control Channel Protection

Organizations face a spectrum of security challenges. Some networks, such as those supporting highly sensitive information and facing a high likelihood of attack, require the most secure solutions that can be deployed, while others require basic VPN, perhaps with encryption of data. Microsoft supports the full spectrum of technology, providing customers with a range of integrated security solutions.

Is Windows NT 4.0-based Virtual Private Networking secure?

Creating a secure computing environment requires attention to security policy and physical security, as well as to secure software. There's no such thing as absolute security. For most business purposes, the cost of breaking PPTP security will likely exceed the value of the information obtained. In this context, Windows NT 4.0 provides a secure infrastructure for Virtual Private Networking (VPN). Initial 40-bit or 128-bit encryption keys are automatically generated for every VPN session, allowing fast, strong data encryption using the RC4 encryption algorithm. In addition, Windows NT 4.0 provides system administrators with the additional tools necessary to secure their installations. This includes integrated user authentication and facilities for enforcing strong password security.

Note that U.S. government policy generally restricts distribution of 128-bit encryption software to sites in the United States and Canada and (under certain circumstances) to banks, financial institutions, and subsidiaries of large U.S. companies in other locations. Given current technology, it is possible to break 40-bit keys within a period of time that grows progressively shorter as technology advances. This is true regardless of the VPN technology under consideration. For this reason, we recommend that customers needing strong data confidentiality use 128-bit keys if possible.

Are there other aspects of security that I should consider when making a decision about a VPN solution?

Yes. Integrated design, ease of implementation and use, and cost are important factors. A poorly designed system may open additional security holes as people try to simplify its operation. For example, a system that requires manual administration of encryption keys may cause people to keep these keys in readily accessible places, reducing the difficulty of an attack. Furthermore, one of the major driving forces behind the corporate adoption of VPN technology has been cost reduction.

Are the security issues different for RAS than for VPN access?

Yes. In particular, the need for encryption is much greater in the VPN case. This is because the data traffic is passing through the Internet, which is more susceptible to eavesdropping than a telephone line. Physical access to the wire or telephone company switch is necessary to tap or redirect a telephone line, and although such incidents have been documented, this access is difficult to achieve. On the other hand, Internet traffic relies on many devices (such as routers and name

servers) en route from your PPTP client to the PPTP server. The sheer number of devices increases the likelihood that an attacker could successfully penetrate one of them in order to redirect or intercept your data traffic.

In addition, a larger number of potential attackers can attempt to break into a VPN server and can launch such attacks more quickly than in the case of a dial-up server. This increases the importance of user authentication for VPN servers and emphasizes the need for strong passwords.

What security features are built into PPTP?

PPTP[1] relies upon security features of the Point-to-Point Protocol (PPP) to provide user authentication and protect the confidentiality of user data. PPP[2, 3,4] is the protocol used to transport data within the PPTP tunnel. PPP authentication methods supported in Windows 9*x* DUN and Windows NT 4.0 RAS include PAP, SPAP, CHAP, and MS-CHAP. Extensible Authentication Protocol (EAP) support will be provided in Windows 2000. Microsoft Point to Point Encryption (MPPE) is supported in Windows 9*x* DUN and Windows NT 4.0 RAS. MPPE uses the RC4 stream cipher.

How is PPTP secured?

PPTP depends upon two proprietary protocols to protect user data at the PPP level: Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP)[5] and MPPE[6].

The newest releases of PPP and PPTP support a new version of MS-CHAP (MS-CHAP version 2)[7], which provides mutual authentication, stronger initial data encryption keys, and separate encryption keys for the transmit and receive paths.

What types of attack are used against VPNs?

Network attacks fall into four basic categories:

- Impersonation

[1] K. Hamzeh, et al., “Point-to-Point Tunneling Protocol--PPTP,” draft-ietf-pppext-pptp-05.txt (work in progress), October 1998.
[2] W. Simpson, "The Point-to-Point Protocol (PPP)," RFC 1661, July 1994.
[3] D. Rand, "The PPP Compression Control Protocol (CCP)," RFC 1962, June 1996.
[4] G. Meyer, "The PPP Encryption Control Protocol (ECP)," RFC 1968, June 1996.
[5] G. Zorn and S. Cobb, “Microsoft PPP CHAP Extensions,” RFC 2433, October 1998.
[6] G. S. Pall and G. Zorn, “Microsoft Point-To-Point Encryption (MPPE) Protocol,” draft-ietf-pppext-mppe-02.txt (work in progress), August 1998.
[7] G. Zorn, “Microsoft PPP CHAP Extensions, Version 2,” draft-ietf-pppext-mschap-v2-00.txt (work in progress), August 1998.

- Integrity
- Disclosure
- Denial of service

Impersonation attacks are those in which an attacker masquerades as another person. The strong authentication methods supported in PPTP can reduce the effectiveness of impersonation attacks.

Successful *integrity* attacks result in the undetected modification of user data; for example, changing the contents of an electronic mail message in transit. Integrity attacks are generally impossible to prevent. The best that can be done is to detect the modification. Digital signatures of various types are useful defenses against integrity attacks.

Disclosure attacks result in the exposure of data to an unintended person. The damage caused by disclosure attacks often depends upon the content of the data revealed: a meeting request may have little value to an opponent, whereas the disclosure of confidential sales projections could be ruinous. The typical defense against disclosure attacks is the use of strong encryption to hide network traffic, which is available in PPTP.

Denial of service attacks are the hardest attacks to defend against, and the easiest to perpetrate. The purpose of these attacks, as the name suggests, is to deny service to valid users. Windows NT 4.0 has been hardened against a number of known denial of service attacks, including teardrop, newtear, and syn flooding.

What has Microsoft done to protect against attacks?

Microsoft takes security very seriously. To defend against attack, we have redesigned MS-CHAP and modified the way that MPPE keys are derived. In the future, we will also be adding strong authentication, integrity protection, and encryption to the PPTP Control Channel. The following discussion describes potential attacks against PPTP and the steps Microsoft has taken to thwart them.

Dictionary Attacks

A *dictionary attack* occurs when an adversary uses a large list of words to try to guess a password. The encrypted password is compared against each word in the list (also encrypted) until a match is found. All password-based authentication methods are vulnerable to dictionary attacks. However, LAN Manager authentication is particularly susceptible, due to the way the password is processed.

To correct this problem, LAN Manager authentication is not supported in MS-CHAP version 2. Only the stronger Windows NT authentication method is supported. The Windows NT authentication method is much

more resistant to dictionary attacks because random data is included in the authentication credentials. The Windows NT authentication method is planned to be supported on Windows 95 and Windows 98, as well as Windows NT.

Server Spoofing

Because only the PPTP client is authenticated, it might be possible for a false PPTP server to masquerade as the real PPTP server. The false server could not decrypt the data transmitted from the client, but it could collect two or more sets of data encrypted under the same encryption key, which could be useful. In addition, it is possible for the false server to request that the user change his password using an obsolete version of the MS-CHAP password changing facility (Change Password Version 1, or CPW1). Because of the way CPW1 was designed, the false server would then be in possession of the user's current password hash, which could be used to impersonate the user to a real PPTP or RAS server.

To correct this problem, MS-CHAP version 2 provides mutual authentication, thus making server spoofing much more difficult. *Mutual authentication* means that not only does the client authenticate to the PPTP server, but also the server authenticates to the client. In addition, support for Change Password version 1 has been removed.

Weak Encryption Keys

The encryption keys used in MPPE are derived from the user's password. If the password is poorly chosen, the resulting encryption key will be relatively weak and easy to break.

To address this issue, Microsoft provided a mechanism for enforcement of strong password security in Windows NT 4.0 Service Pack 2. The system administrator can force all users to change passwords (one time or on a scheduled basis). During the password change operation, the system can inspect the user's choice of password to ensure that it meets minimum requirements in length and randomness. However, it's up to users and administrators to make sure that the tool is used and to keep security in mind.

Repeated Use of the Same Encryption Key

When MS-CHAP version 1 is used for authentication and 40-bit encryption is negotiated, the same initial encryption key is used for each PPTP session begun while the user's password is the same. This is because only the password is used to derive the initial 40-bit key, without any other information unique to the session itself. 128-bit keys do not have this problem, because session-specific data is used to derive them. However, the same key is used for both sending and receiving data, which means that some data is encrypted under the same key in any

case.

In MS-CHAP version 2, data unique to the current session is incorporated into all the encryption keys, both 40- and 128-bit. Separate encryption keys are derived for both the send and receive directions of the link.

MPPE Key Synchronization

Originally, MPPE changed the encryption key every 256 packets or whenever a packet was lost. If packet loss was detected by the receiver, it sent an unauthenticated request to the sender to change the key in order to resynchronize. This behavior made it possible for an attacker to mount a denial of service attack by either modifying the counter in an MPPE packet or forging a resynchronization request.

To address this issue, in PPTP, by default, the MPPE keys are now changed on every packet. This change defeats the key resynchronization attack.

Bit-Flipping

MPPE uses the RC4 encryption algorithm, invented at RSA Laboratories. One of the qualities of RC4 is that it provides no inherent support for the protection of data integrity. This means that it is possible to randomly *flip* bits in the PPTP data stream without the changes being detected.

This issue will be addressed in a forthcoming release by redesigning the PPTP data channel to include integrity protection.

PPP Negotiation Spoofing

The PPP negotiations between the PPTP client and server are unencrypted and unauthenticated. For this reason, it is possible for an adversary to spoof PPP negotiation packets, such as those containing the address of the DNS server or the internal IP address to be used by the client. In order to do this, it would be necessary to be able to insert or modify packets in the PPTP data stream, however.

This issue will be addressed in a forthcoming release by adding per-packet authentication and integrity protection to the PPTP data channel.

Passive Monitoring

By monitoring the PPTP control and data channels during the tunnel initialization, some information about the PPTP server and client can be obtained. This information includes the client and server IP addresses, the internal IP address assigned to the client side of the PPTP tunnel, the addresses of any internal DNS servers given to the client, and the client user name.

This issue will be addressed in a forthcoming release by redesigning the PPTP data channel.

How important is good password security?

Because PPTP security is password-based in Windows NT 4.0, the choice of a good password is an important security consideration. Regardless of the key length chosen (40- or 128-bit), the true size of key space is governed by the randomness of the password. The English language only supplies about 1.3 bits of randomness per character.[8] Thus, a 10-character English password is thus only equivalent to a 13-bit key, which is far too small. In contrast, a 10-character password composed of a random collection of upper and lower case letters, numbers, and punctuation would provide enough randomness for a 40-bit key. Thus, well-chosen passwords can be converted into reasonably secure encryption keys, whereas poorly chosen passwords cannot.

In practice, it is advisable to provide password randomness comparable to the key length chosen. Thus, when 128-bit encryption keys are used, longer passwords should generally be required. In Windows NT 4.0, passwords may have a maximum length of 14 characters.

Poorly chosen passwords include those that are:

- Made up solely from dictionary words.
- Only one case (upper or lower).
- Created from names of people or things that you like (Your mother's maiden name is not a good password—you'd be surprised how many people know it!).

Well-chosen passwords:

- Contain at least one number and one symbol (for example, *?*) in the middle of the word.
- Appear to be *gobbledygook* to the casual observer.
- Do not contain dictionary words or proper names.

Windows NT 4.0, Service Pack 2, provides facilities to enforce good password security.

Are IPSec-based VPNs more secure than PPTP-based VPNs?

Not necessarily. As with any VPN solution, the security of an IPSec-based VPN solution is dependent upon aspects of the implementation. For example, the security of a public key-based VPN solution is only as good as the mechanisms used to protect the user's private keys.

Most of today's IPSec[9, 10, 11] implementations support public key certificates. In theory, these can generate stronger encryption keys than

[8] T.M. Cover and R.C. King, "A Convergent Gambling Estimate of Entropy," IEEE Transactions on Information Theory, v. IT-24, n. 4, July 1978, pp. 413-421.

[9] R. Atkinson and S. Kent, "Security Architecture for the Internet Protocol," draft-ietf-ipsec-arch-sec-05.txt (work in progress), May 1998.

mechanisms based on shared passwords. However, most IPSec implementations rely on machine certificates and consequently, do not authenticate user credentials. This means that access is granted based on authentication of the machine endpoints; the identity of the user may not be known. However, in the case of VPN access, it is typically required that authorization be supported. In the case when a client machine may be accessed by more than one user (such as with roaming users or multiuser machines), authorizing access to the corporate network purely based on machine certificates creates a security loophole.

Are L2TP-based VPNs more secure than PPTP-based VPNs?

Not necessarily. As with any VPN solution, the security of an L2TP[12]-based VPN solution is dependent upon aspects of the implementation. Standards-compliant L2TP-based VPNs that require security use IPSec to provide confidentiality as well as message integrity protection[13]. In such implementations, PPP-based authentication is typically used along with IPSec, so that user authorization can be provided. Consequently, L2TP-based VPNs using IPSec can be secured in a variety of scenarios.

Is VPN outsourcing secure?

In VPN outsourcing, security becomes the responsibility of the service provider. Data or even passwords may be available to the provider in unencrypted form. In such a situation, it is very important that the VPN provider be trustworthy, because it will control the devices through which your data flows. Consequently, it is important to have a solid contract with a reputable provider.

Is a server-to-server based VPN solution more secure than a client-server solution?

Various factors may help to make a server-to-server VPN more secure. For example, the passwords used can be longer, more random, and need not make sense, because they will typically be stored on disk. These potential benefits are useful if all VPN traffic can be funneled through these servers. A server-based solution also dictates a requirement for strong physical security to protect the servers.

---

[10] S. Kent and R. Atkinson, "IP Authentication Header," draft-ietf-ipsec-auth-header-06.txt (work in progress), May 1998.
[11] S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," draft-ietf-ipsec-esp-v2-05.txt (work in progress), May 1998.
[12] K. Hamzeh, et al., "Layer Two Tunneling Protocol—L2TP," draft-ietf-pppext-l2tp-10.txt (work in progress), April 1998.
[13] B. Patel and B. Aboba, "Securing L2TP Using IPSEC," draft-ietf-pppext-l2tp-security-02.txt, May 1998.

FOR MORE INFORMATION

What are smart cards?

Smart cards are small devices about the size of credit cards. The cards contain a CPU and a small amount of random access memory, and have various defenses against mechanical and electrical tampering. They are commonly used to store authentication credentials (like public key certificates), encryption keys, account information, and so forth. Most smart cards will not function without a PIN or other password to unlock their contents. The most useful cards implement encryption algorithms on board, so that the encryption keys never leave the smart card.

Does Microsoft support smart card authentication for VPNs?

Smart card authentication is not supported in Windows NT 4.0. However, in Windows 2000, Microsoft plans to support smart card authentication for logging on to Windows NT, and use with RAS, IPSec, L2TP, and PPTP.

What are token cards?

Token cards from different vendors work in a variety of ways, but they are all basically hardware password generators. For example, some cards have a small LCD display and a keypad like a calculator. The user enters a numeric PIN and the card displays a numeric passcode, which is then used as a password. Normally, token cards are designed so that they will only produce a given passcode once. Token cards work great for dial-up applications (like RAS) or host authentication. Because network applications of token cards are usually client/server-based, token cards (and other one-time password schemes) can be vulnerable to eavesdropping and replay attacks.

What are the tradeoffs between smart cards, token cards, and password-based security?

Token cards are often inconvenient and are usually proprietary. Generally, token card authentication servers do not generate encryption keys to be used for protecting user data on the network. Token card solutions typically support initial authentication, but not data encryption or message integrity protection. It is possible for initially authenticated sessions to be subsequently hijacked or snooped on the wire. Consequently, customers desiring data confidentiality or hijack protection are advised to use solutions providing for key generation, such as public key-based smart cards. Public key smart cards are very convenient and secure, but they are expensive right now and few remote access packages support their use.

For the latest information on Windows NT Server, check out our World Wide Web site at http://www.microsoft.com/ntserver and the Windows NT

Server Forum on the Microsoft Network (GO WORD: MSNTS).

Other sites to visit include:

The Windows NT Communication Services home page:

http://www.microsoft.com/communications

The Microsoft security Web site:

http://www.microsoft.com/security

For information on PPTP:

http://www.microsoft.com/communications/pptp.htm

For information on Microsoft Routing and Remote Access:

http://www.microsoft.com/communications/routing&ras.htm

For information on smart cards:

http://www.microsoft.com/smartcard/

For information on the Windows platform:

http://www.microsoft.com/windows/

For information on developer information and tools:

http://www.microsoft.com/msdn/

For a collection of documents about Windows NT Server:

http://www.microsoft.com/ntserver

For information on the beta program of Windows 2000:

http://ntbeta.microsoft.com